
DRAFT



SUMMARY TABLE FOR:
"Internet PKI, Certificate
Management Protocols,"
draft-ietf-pkix-ipki3cmp-08.txt,
May 1998



25 June 1998

Prepared by:

Center for Standards
Defense Information Systems Agency

DRAFT

This Page left intentionally blank.

Disclaimer

Persons and organizations use this document at their own risk.

This document is for information only. If there is any conflict between this document and the source document, the source document takes precedence.

The U. S. Federal Government does NOT provide any guarantee as to the accuracy of this document. This document is NOT a request for proposal, a request for bid, or a modification to any contract currently held with the U. S. Federal Government.

Distribution of this document is unlimited.

Acronyms

CA	- Certification Authority
D-H	- Diffie-Hellman
EE	- End-Entity
IKA	- Initial Authentication Key
KAK	- Key Agreement Key
MAC	- Message Authentication Code
OWF	- One Way Function
PSE	- Personal Security Environment
RA	- Registration Authority

This Page left intentionally blank.

STATUS CODES: M – MANDATORY, O – OPTIONAL, C – CONDITIONAL

SECTION	FEATURE	STATUS	REMARKS
1	PKI MANAGEMENT OVERVIEW		
1.1	PKI Management Model		
1.2	Definitions of PKI Entities		
1.2.1	Subjects and End Entities	M	
	Personal Security Environment	M	
	Secure local access to	M	
	Own name	M	
	Own private key	M	
	Name of trusted CA	M	
	Trusted CA's public key	M	
	Other information	O	
1.2.2	Certification Authority	M	
1.2.3	Registration Authority	O	
1.3	PKI Management Requirements	M	
	Conformance to ISO 9594-8 standard and certificate extensions	M	
	Conformance to other Internet PKI specifications	M	
	Key pair updating without affecting other key pairs	M	
	Minimal use of confidentiality	M	
	Support use of different cryptographic algorithms	M	
	Support key pair generation at EE	M	
	Support key pair generation at RA	M	
	Support key pair generation at CA	M	
	Key generation occurs wherever key is first presented	M	
	Support publication of certificates by EE	M	
	Support publication of certificates by RA	M	
	Support publication of certificates by CA	M	
	Support certified end-entities to request certificate revocation	M	
	Maintain level of protection from denial-of-service attacks	M	
	Usable over mail	M	
	Usable over http	M	
	Usable over TCP/IP	M	
	Usable over ftp	M	
	EE acceptance of certificates conforming to issuing CA's policy	M	
	RA acceptance of certificates conforming to issuing CA's policy	M	
	CA acceptance of certificates conforming to issuing CA's policy	M	
	Issuing CA hold publication of certificate pending acceptance by requester	O	
	Scheduled, graceful CA key update	M	
	CA key compromised	C	
	All domain entities re-initialize	M	
	EE accepts certificates verifiable with issuing CA's old public key	M	

SECTION	FEATURE	STATUS	REMARKS
	EE accepts certificates issued under issuing CA's new private key	M	Case: old CA public key is hardwired into EE's crypto equipment
	End-entities use the same protocol to communicate with RAs or CAs	M	CA may perform RA duties.
	Maintain separate key pairs for RA and CA functions	M	
	EE can obtain certificate containing a given public key value after demonstrating possession of private key value	M	ref. 2.3
	PKI Management Operations	M	
	CA establishment	M	ref. 4.1, 4.3
	EE initialization	M	ref. 2.1, 3.3.1, 3.3.2, 4.7
	Certification	M	
	Initial registration/certification	M	ref. 2.2, 3.3.3, 3.3.4
	Key pair update	M	ref. 3.3.5, 3.3.6, 4.9
	Certificate update	M	ref. 4.8, Upon expiration
	CA key pair update	M	ref. 2.4, 3.3.13, 4.2
	Cross-certification request	M	ref. 3.3.11, 3.3.12, 4.6 a.k.a. CA-certificate in X.509
	Subject CA distinct	M	
	Issuer CA distinct	M	
	SubjectPublicKeyInfo binds subject CA's signing key pair	M	
	Mutual cross-certificates issued	O	
	Cross-certification update	M	ref. 4.8
	Certificate/CRL discovery operations	M	
	Certificate publication	M	ref. PKIXLDAP, sec. 3.3.13-16
	CRL publication	M	ref. PKIXLDAP, sec. 3.3.13-16, 4.4
	Recovery operations	M	EE has lost PSE
	Key pair recovery	M	ref. 3.3.7, 3.3.8
	CA backs up client key materials	O	
	RA backs up client key materials	O	
	OR a key backup system associated with a CA or RA	O	
	Protocol to exchange backed up key materials	M	
	Revocation Operations	M	ref. 3.3.15
	Revocation request	M	ref. 3.3.9, 3.3.10
	PSE operations	M	PKIMessage (CertRepMessage)
	On-line implementation	O	
	Off-line implementation	O	
2	ASSUMPTIONS AND RESTRICTIONS	M	
2.1	End Entity Initialization	M	
	Request information re PKI functions supported	M	
	Securely acquire a copy of the relevant root CA public key(s)	M	

SECTION	FEATURE	STATUS	REMARKS
2.2	Initial Registration/Certification	M	Dependent on CA policies and EE type. EE has had no previous contact with PKI
2.2.1	Criteria Used	M	
2.2.1.1	Initiation of Registration/Certification	M	
	Occurs with generation of first PKI message related to EE	M	ref. 3.1
	Generated at CA	O	
	Generated at RA	O	
	Generated at EE	O	
2.2.1.2	End Entity Message Origin Authentication	O	Authentication of CA/RA messages achieved by use of their public key
	CA/RA authenticate received EE messages	O	
	Out-of-band distribution of initial authentication key and reference value	O	
	Out-of-band authentication	O	
2.2.1.3	Location of Key Generation		
	Generated with first occurrence in PKIMessage	M	ref. 3.1
	Generated at CA	O	
	Generated at RA	O	
	Generated at EE	O	
2.2.1.4	Confirmation of Successful Certification	O	Provides additional assurance
	EE confirms receipt of certificate by secure means	O	
2.2.2	Mandatory Schemes	M	
	Support of other schemas	O	
2.2.2.1	Centralized Scheme	O	
	Initiation occurs at certifying CA	M	ref. 2.2.1.1
	On-line message authentication	O	ref. 2.2.1.2
	Key generation occurs at certifying CA	M	ref. 2.2.1.3
	Confirmation message	O	ref. 2.2.1.4
	CA message to EE contains entire PSE	M	
	Out-of-band authentication by EE	M	
	Out-of-band provision of decryption key to EE	M	
2.2.2.2	Basic Authenticated Scheme	M	
	Initiation occurs at EE	M	ref. 2.2.1.1
	On-line message authentication	M	ref. 2.2.1.2
	Key generation occurs at EE	M	ref. 2.2.1.3
	Confirmation message	M	ref. 2.2.1.4
	RA/CA revokes issued certificate on confirmation failure	M	
	Out-of-band distribution of IAK from RA/CA to EE	M	
	Out-of-band distribution of reference value from RA/CA to EE	M	
2.3	Proof of Possession (POP) of Private Key	M	CARAs must confirm the EE's possession of a private key paired to the public key bound in the certificate
	Out-of-band procedures	O	
	In-band procedures	O	

SECTION	FEATURE	STATUS	REMARKS
	RA confirms verification of EE POP to CA	O	
	CA only permitted to verify EE POP	O	
	Different procedures for key types	M	
	Signature keys	M	ref. 2.3.1
	Encryption keys	M	ref. 2.3.2
	Key Agreement keys	M	ref. 2.3.3
	Multiple purpose keys	O	ref. 2.3.1, .2, .3
2.3.1	Signature Keys	M	
	EE signs a value using its private key	O	
2.3.2	Encryption Keys	M	
	EE provides private key to CA/RA	O	
	EE decrypts value using private key	O	ref. 3.2.8
	Direct Method	O	
	EE immediately responds to random challenge from CA/RA	M	
	Indirect Method	O	RECOMMENDED
	CA issues a certificate encrypted by the EE's public key	M	CA issues a certificate which only intended EE can use
	EE proves its ability to decrypt the certificate in confirmation message	M	Returns decrypted certificate?
2.3.3	Key Agreement Keys	M	
	EE and CA/RA establish shared secret key	M	
	Encrypted exchange verifies POP	M	
	CA generates short-term key pair within parameters	C	
	CA certifies keys without restrictions	O	
2.4	Root CA Key Update	O	
	CA is root CA for some EE(s)	M	
	Certificates made available using X.500 directory	C	
	CA generates two additional cACertificate attributes	M	
	Protects new public key with old private key	M	Supports EE that acquire CA public keys via out-of-band means
	Protects old public key with new private key	M	EE can obtain old public key using new public key in order to decrypt what was encrypted with the old private key
	Support of version 1 certificates	M	
	X.509v3 extensions prohibited	M	
	Validity period of a CA key pair is greater than any certificate issued using that key pair	M	
	EE acquires new CA public key upon expiration of last certificate issued using old CA private key	M	Doesn't the EE get the new CA public key when the first certificate expires, not the last?

SECTION	FEATURE	STATUS	REMARKS
	Out-of-band means	M	Distributing CA public keys by only out-of-band means seems to be an onerous requirement to mandate. Is this possibly an optional requirement? Do other pkix specifications, permit distributions in-band?
2.4.1	CA Operator Actions	M	
	To change the CA key	M	
	CA generates new key pair	M	
	CA creates a certificate containing old public key signed with new private key (OldWithNew)	M	Old CA public key required only for non-repudiation after all CA's EEs have new CA public key.
	Certificate validity period	M	
	Start at the generation time of the old key pair	M	
	End at the expiration time of the old public key	M	
	CA creates a certificate containing new public key signed with old private key (NewWithOld)	M	
	Certificate validity period	M	
	Start at the generation time of the new key pair	M	
	End when all the CA's EEs possess the new CA public key	M	
	The expiration time of the old public key at latest	M	
	CA creates a certificate containing new public key signed with new private key (NewWithNew)	M	
	Certificate validity period	M	
	Start at the generation time of the new key pair	M	
	End at the time of the next key update	M	
	Publish certificates	M	
	Via directory	O	
	Via other means	O	
	Make new CA public key available to EEs	M	Old CA private key is no longer required.
	Out-of-band means	O	Conflict with 2.4?
	In-band means	O	Conflict with 2.4?
2.4.2	Verifying Certificates	M	
2.4.2.1	Verification in Cases 1, 4, 5 and 8	M	
	Case 1: Repository contains NEW and OLD public keys	C	
	PSE Contains NEW public key	&	
	Signer's certificate is protected using NEW public key	&	
	Signer's public key can be verified using verifier's local copy of the CA public key	M	
	Case 4: Repository contains NEW and OLD public keys	C	
	PSE Contains OLD public key	&	

SECTION	FEATURE	STATUS	REMARKS
	Signer's certificate is protected using OLD public key	&	
	Signer's public key can be verified using verifier's local copy of the CA public key	M	
	Case 5: Repository contains only OLD public key	C	Occurs if CA has issued both the signer's and verifier's certificates during the time between the generation of a new key pair and when the directory attributes are updated.
	PSE Contains NEW public key	&	
	Signer's certificate is protected using NEW public key	&	
	Signer's public key can be verified using verifier's local copy of the CA public key	M	
	Case 8: Repository contains only OLD public key	C	Occurs during the time between the generation of a new key pair and when the directory attributes are updated.
	PSE Contains OLD public key	&	
	Signer's certificate is protected using OLD public key	&	
	Signer's public key can be verified using verifier's local copy of the CA public key	M	
2.4.2.2	Verification in Case 2	M	Occurs when CA has issued signer's certificate then changed key and issued the verifier's certificate.
	Repository contains NEW and OLD public keys	C	
	PSE Contains NEW public key	&	
	Signer's certificate is protected using OLD public key	&	
	Verifier gets the CA's OLD public key to verify signer's certificate by	M	
	Obtaining OldWithNew certificate from the directory	M	
	Determine based on validity periods	M	
	Use local copy of NEW CA public key to verify it	M	
	If verified, use OLD CA public key in certificate	M	
	Verification failure	O	UNSPECIFIED
2.4.2.3	Verification in Case 3	M	Occurs when CA has issued verifier's certificate then changed key and issued the signer's certificate.
	Repository contains NEW and OLD public keys	C	
	PSE Contains OLD public key	&	
	Signer's certificate is protected using NEW public key	&	
	Verifier gets the CA's NEW public key to verify signer's certificate by	M	

SECTION	FEATURE	STATUS	REMARKS
	Obtaining NewWithOld certificate from the directory	M	
	Determine based on validity periods	M	
	Use local copy of OLD CA public key to verify it	M	
	If verified, use NEW CA public key in certificate	M	
	Verification failure	O	UNSPECIFIED
2.4.2.4	Failure of Verification in Case 6	M	Occurs when CA has issued the verifier's PSE containing new key without updating the directory attributes. Verifier has no means to get trustworthy copy of CA's old public key. CA held at fault.
	Repository contains only OLD public key	C	
	PSE Contains NEW public key	&	
	Signer's certificate is protected using OLD public key	&	
	Verification failure	M	
2.4.2.5	Failure of Verification in Case 7	M	Occurs when CA has issued the signer's certificate protected with the new key without updating the directory attributes. Verifier has no means to get trustworthy copy of CA's new public key. CA held at fault.
	Repository contains only OLD public key	C	
	PSE Contains OLD public key	&	
	Signer's certificate is protected using NEW public key	&	
	Verification failure	M	
2.4.3	Revocation – Change of CA Key	M	Change of keys also impact revocation checks. CA may sign CRL with a newer key than found in EE's PSE
	Verification in Cases 1	M	ref. 2.4.2.1
	Verification in Cases 2	M	ref. 2.4.2.2
	Verification in Cases 3	M	ref. 2.4.2.3
	Verification in Cases 4	M	ref. 2.4.2.1
	Verification in Cases 5	M	ref. 2.4.2.1
	Failure of Verification in Case 6	M	ref. 2.4.2.4
	Failure of Verification in Case 7	M	ref. 2.4.2.5
	Verification in Cases 8	M	ref. 2.4.2.1
3	DATA STRUCTURES	M	For PKI management messages
3.1	Overall PKI Messages	M	
	SEQUENCE	M	
	header PKIHeader	M	ref. 3.1.1 Common information
	body PKIBody	M	ref. 3.1.2 Message specific information

SECTION	FEATURE	STATUS	REMARKS
	protection [0] PKIProtection	O	ref. 3.1.3 Contains bits that protect the PKI message.
	extraCerts [1] SEQUENCE SIZE of Certificate	O	Certificates of possible use to the recipient
3.1.1	PKI Message Header	M	Addressing and transaction identification
	SEQUENCE	M	
	pvno INTEGER (1)	M	Fixed at one for this specification version
	sender GeneralName	M	ref. PKIX1, sec. 4.2.1.7 Sender's name, usable to verify the message's protection.
	NULL field when sending entity knows nothing about the sender	M	Entity may not know its own DN, etc. NULL field is a SEQUENCE OF RDNs of zero length.
	senderKID field present	M	Provide a reference to the receiver that indicates the appropriate shared secret information that verifies the message
	recipeint GeneralName	M	ref. PKIX1, sec. 4.2.1.7 Recipient's name, usable to verify the message's protection.
	messageTime [0] GeneralizedTime	O	Time sender created the message. Meaningful on reception?
	protectionAlg [1] AlgorithmIdentifier	O	Specifies the algorithm use to protect the message
	Omit when PKIProtection not supplied	M	
	Supply when PKIProtection supplied	M	
	senderKID [2] KeyIdentifier	O	Indicates keys used to protect message
	recipKID [3] KeyIdentifier	O	Indicates keys used to protect message
	This field only present if D-H keys protect the message	M	
	transactionID [4] OCTET STRING	M	The same in corresponding request, response and confirmation messages.
	senderNonce [5] OCTET STRING	O	Protects against replay attacks. Inserted by sender.
	recipNonce [6] OCTET STRING	O	Protects against replay attacks. Nonce previously inserted in a related message by the intended recipient.

SECTION	FEATURE	STATUS	REMARKS
	freeText [7] PKIFreeText	O	Use to send human-readable message to recipient in any language.
	SEQUENCE SIZE OF UTF8String	M	First language used in the sequence indicates language for replies.
	generallnfor [8] SEQUENCE SIZE OF InfoTypeAndValue	O	Use to send additional machine-processable data
3.1.2	PKI Message Body		Message-specific body elements
	CHOICE	M	ref. 3.3
	ir [0] CertReqMessages	O	Initialization Request, ref. 3.3.1
	ip [1] CertRepMessage	O	Initialization Response, ref. 3.3.2
	cr [2] CertReqMessages	O	Certification Request, ref. 3.3.3
	cp [3] CertRepMessage	O	Certification Response, ref. 3.3.4
	p10cr [4] CertificationRequest	O	the PKCS #10 certification request (ref. [PKCS10])
	popdecc [5] POPODecKeyChallContent	O	pop Challenge
	popdecr [6] POPODecKeyRespContent	O	pop Response
	kur [7] CertReqMessages	O	Key Update Request, ref. 3.3.5
	kup [8] CertRepMessage	O	Key Update Response, ref. 3.3.6
	krr [9] CertReqMessages	O	Key Recovery Request, ref. 3.3.7
	krp [10] KeyRecRepContent	O	Key Recovery Response, ref. 3.3.8
	rr [11] RevReqContent	O	Revocation Request Response, ref. 3.3.9
	rp [12] RevRepContent	O	Revocation Response, ref. 3.3.10
	ccr [13] CertReqMessages	O	Cross-Cert. Request, ref. 3.3.11
	ccp [14] CertRepMessage	O	Cross-Cert. Response, ref. 3.3.12
	ckuann [15] CAKeyUpdAnnContent	O	CA Key Update Ann., ref. 3.3.13
	cann [16] CertAnnContent	O	Certificate Ann., ref. 3.3.14
	rann [17] RevAnnContent	O	Revocation Ann., ref. 3.3.15
	crlann [18] CRLAnnContent	O	CRL Announcement, ref. 3.3.16
	conf [19] PKIConfirmContent	O	Confirmation, ref. 3.3.17
	nested [20] NestedMessageContent	O	Nested Message
	genm [21] GenMsgContent	O	General Message, ref. 3.3.18

SECTION	FEATURE	STATUS	REMARKS
	genp [22] GenRepContent	O	General Response, ref. 3.3.19
	error [23] ErrorMsgContent	O	Error Message, ref. 3.3.20
3.1.3	PKI Message Protection	O	External protection permitted, e.g., PKCS #7 and RFC 1847. Parameter recommended for cases of initial registration, key-recovery, or any other "bootstrapping" process.
	PKIProtection ::= BIT STRING	M	
	ProtectedPart ::= SEQUENCE	M	DER encoded input to calculation of PKIProtection
	header PKIHeader	M	ref. 3.1.1
	body PKIBody	M	ref. 3.1.2
	Message Authentication Code (MAC) use	O	PKIProtection will contain a MAC value keyed with a derived symmetric key. Protection algorithms will vary.
	Sender and Recipient share secret information	O	
	PasswordBasedMac ::= OBJECT IDENTIFIER	M	1 2 840 113533 7 66 13 protection algorithm
	PBMPParameter ::= SEQUENCE	M	
	salt OCTET STRING	M	Value appended to shared secret input.
	owf AlgorithmIdentifier	M	ref. PKIX1, sec. 4.1.1.2, Identifier for OWF Hash, RECOMMEND SHA-1 (ref. PKIX1, sec. 7.1.3)
	First input is salted secret.	M	
	Subsequent inputs are previous outputs.	M	
	Final output is BASEKEY of size "H"	M	Used to form the symmetric key
	iterationCount INTEGER	M	Number of times OWF is applied.
	mac AlgorithmIdentifier	M	ref. PKIX1, sec. 4.1.1.2, MAC or HMAC
	Algorithm requires a K-bit key	O	
	K <= H then MSB of BASEKEY used	M	
	K > H	M	
	then all of BASEKEY used for H's MSB	M	
	OWF ("1" BASEKEY) used for H's next MSB	M	Number is ASCII byte encoded. represents concatenation
	OWF ("n" BASEKEY) used for H's next MSB	M	Continued until all K bits have been derived.

SECTION	FEATURE	STATUS	REMARKS
	Sender and receiver possess D-H certificates with compatible D-H parameters	O	EE must generate a symmetric key based on its private D-H key value and the receiver's D-H public key.
	DHBasedMac ::= OBJECT IDENTIFIER	M	1 2 840 113533 7 66 30
	DHBMPParameter ::= SEQUENCE	M	
	owf AlgorithmIdentifier	M	ref. PKIX1, sec. 4.1.1.2, Identifier for OWF Hash, RECOMMEND SHA-1 (ref. PKIX1, sec. 7.1.3)
	Apply to D-H result	M	
	Output is BASEKEY of size "H"	M	
	mac AlgorithmIdentifier	M	ref. PKIX1, sec. 4.1.1.2, MAC or HMAC
	Algorithm requires a K-bit key	O	
	K <= H then MSB of BASEKEY used	M	
	K > H	M	
	then all of BASEKEY used for H's MSB	M	
	OWF ("1" BASEKEY) used for H's next MSB	M	Number is ASCII byte encoded. represents concatenation
	OWF ("n" BASEKEY) used for H's next MSB	M	Continued until all K bits have been derived.
	Sender possesses a signature key pair	O	
	PKIProtection contains signature value	M	
	protectionAlg is AlgorithmIdentifier for a digital signature	M	ref. PKIX1, sec. 7.2
	Multiple protection	O	
	NestedMessageContent ::= PKIMessage	M	Entire message sent within new PKI message.
3.2	Common Data Structures	M	Used in PKIBody
3.2.1	Requested Certificate Contents	M	ref. CRMF for syntax. A data structure to specify the certificate content.
	Message originator indicates some fields it wishes present in the certificate being issued to it.	M	
	CA has discretion over fields included in the certificate regardless of originators request	M	
3.2.2	Encrypted Values		ref. CRMF for syntax. A data structure to send encrypted values in PKI messages.
	Use when PKI message contains private key	M	
	Use when PKI message contains certificate	M	
	Sender and receiver can encrypt/decrypt	M	
	Sender and receiver have or can generate a shared secret key	O	
	Receiver has private key for decryption	C	
	encSymmKey contains session key encrypted with receiver's public key	O	

SECTION	FEATURE	STATUS	REMARKS
3.2.3	Status Codes and Failure Information for PKI Messages	M	A data structure that provides status information in the response messages.
	PKIStatusInfo ::= SEQUENCE	M	
	status PKIStatus	M	
	PKIStatus ::= INTEGER	M	
	granted (0)	O	Requester gets exactly what they asked for
	grantedWithMods (1)	O	Requester gets something like what they asked for. They are responsible for ascertaining the differences
	rejection (2)	O	Request denied. More information elsewhere in the message.
	waiting (3)	O	The request body part has not yet been processed, expect to hear more later.
	revocationWarning (4)	O	This message contains a warning that a revocation is imminent.
	revocationNotification (5)	O	A revocation has occurred.
	keyUpdateWarning (6)	O	Update already done for the oldCertId specified in the key update request message
	statusString PKIFreeText	O	ref. 3.1.1
	failInfo PKIFailureInfo	O	Additional information providing reason for failure.
	PKIFailureInfo ::= BIT STRING	M	
	badAlg (0)	O	Unrecognized or unsupported Algorithm Identifier.
	badMessageCheck (1)	O	Integrity check failed (e.g., signature did not verify).
	badRequest (2)	O	Transaction not permitted or supported.
	badTime (3)	O	messageTime was not sufficiently close to the system time, as defined by local policy.
	badCertId (4)	O	No certificate could be found matching the provided criteria.
	badDataFormat (5)	O	The data submitted has the wrong format.
	wrongAuthority (6)	O	The authority indicated in the request is different from the one creating the response token.

SECTION	FEATURE	STATUS	REMARKS
	incorrectData (7)	O	The requester's data is incorrect (used for notary services).
	missingTimeStamp (8)	O	When the timestamp is missing but should be there (by policy).
3.2.4	Certificate Identification	M	ref. CRMF for syntax. A data structure that provides the identification of particular certificates.
3.2.5	“Out-of-Band” Root CA Public Key	M	A data structure to support out-of-band distribution of current root CA public key.
	Root CA directly distributes its self-signed certificate out-of-band	O	
	OOBCert ::= Certificate	M	ref. PKIX1, sec. 4
	Signature field verified by use of SubjectPublicKeyInfo field	M	Self-signed certificate
	Subject and Issuer field are identical	M	
	Subject field NULL	O	
	subjectAltNames and issuerAltNames extensions are present and identical	M	
	Key identifiers for subject and issuer are identical	M	
	All other extensions are suitable to self-signed certificate	M	keyCertSign bit of Key Usage extension? Others?
	Root CA makes its self-signed certificate available on-line and distributes a hash of it out-of-band	O	Anyone who has securely received the hash value can verify the on-line self-signed certificate.
	OOBCertHash ::= SEQUENCE	M	
	hashAlg [0] AlgorithmIdentifier	O	
	certId [1] CertId	O	ref. CRMF for syntax
	hashVal BIT STRING	M	Calculated over the self-signed certificate with the identifier certId.
3.2.6	Archive Options	O	ref. CRMF for syntax. A data structure to request the PKI to archive a private key value.
3.2.7	Publication Information	O	ref. CRMF for syntax. A data structure to request the PKI to publish a certificate.
3.2.8	Proof of Possession Structures	O	ref. CRMF for syntax. A data structure used to demonstrate possession of a private key.
	Certification request for a signing key pair	O	A verification certificate
	POPOSigningKeyInput ::= SEQUENCE	M	
	authInfo CHOICE	M	
	sender [0] GeneralName	O	ref. PKIX1, sec. 4.2.1.7
	publicKeyMAC [1] PKMACValue	O	
	publicKey SubjectPublicKeyInfo	M	

SECTION	FEATURE	STATUS	REMARKS
	Certification request for an encryption key pair	O	An encryption certificate
	Include encrypted private key in CertRequest	O	ref. 3.2.6
	CA returns an encrypted certificate	O	ref. 2.3.2, indirect method
	Encryption under randomly-generated symmetric key and	M	
	Symmetric key encrypted under requester's public key	M	
	EE MACs the PKIConfirm message	M	ref. 3.1.3
	PasswordBasedMAC	M	
	Key derived from symmetric key provided by CA	M	
	More than one CertReqMsg included in PKIMessage	O	
	CA uses a different symmetric key for each	M	
	EE concatenates all symmetric keys for MACing	M	
	EE engages in challenge-response	O	ref. 2.3.2, direct method Typical use: CA trusts RA. RA certifies POP and then makes a request to the CA in behalf of EE.
	Performed between CertReqMessages and CertRepMessage	M	
	CA creates certificate only on completion of POP	M	
	One Challenge per encryption key certification request.	M	
	Responses are in same order as the requests appear in CertReqMessages.	M	
	POPODecKeyChallContent ::= SEQUENCE OF	M	
	Challenge ::= SEQUENCE	M	
	owf AlgorithmIdentifier	C	ref. PKIX1, sec. 4.1.1.2, Identifier for OWF hash, ref. PKIX1, sec. 7.1
	First Challenge	M	
	Subsequent Challenges	O	
	Not present, owf used in previous challenge reused	M	
	witness OCTET STRING	M	
	Result of OWF to randomly-generated INTEGER "A"	M	
	Unique INTEGER used for each Challenge	M	
	challenge OCTET STRING	M	
	Encryption of Rand under requester's public key	M	
	Rand ::= SEQUENCE	M	
	int INTEGER	M	INTEGER "A"
	sender GeneralName	M	From PKIHeader, ref. 3.1.1
	POPODecKeyRespContent ::= SEQUENCE OF INTEGER	M	
	INTEGER "A" returned to sender	M	

SECTION	FEATURE	STATUS	REMARKS
	Certification request for an key agreement key (KAK) pair	O	
	Include encrypted private key in CertRequest	O	ref. 3.2.6
	CA returns an encrypted certificate	O	ref. 2.3.2, indirect method
	Encryption under symmetric key derived from CA's private KAK and requester's public key	M	
	EE MACs the PKIConfirm message	M	ref. 3.1.3
	PasswordBasedMAC	M	
	Key derived from symmetric key provided by CA	M	
	More than one CertReqMsg included in PKIMessage	O	
	CA uses a different symmetric key for each	M	
	EE concatenates all symmetric keys for MACing	M	
	EE engages in challenge-response	O	ref. 2.3.2, direct method Typical use: CA trusts RA. RA certifies POP and then makes a request to the CA in behalf of EE.
	Performed between CertReqMessages and CertRepMessage	M	
	CA creates certificate only on completion of POP	M	
	One Challenge per encryption key certification request.	M	
	Responses are in same order as the requests appear in CertReqMessages.	M	
	POPODecKeyChallContent ::= SEQUENCE OF	M	
	Challenge ::= SEQUENCE	M	
	owf AlgorithmIdentifier	C	ref. PKIX1, sec. 4.1.1.2, Identifier for OWF hash, ref. PKIX1, sec. 7.1
	First Challenge	M	
	Subsequent Challenges	O	
	Not present, owf used in previous challenge reused	M	
	witness OCTET STRING	M	
	Result of OWF to randomly-generated INTEGER "A"	M	
	Unique INTEGER used for each Challenge	M	
	challenge OCTET STRING	M	
	Encryption of Rand using PreferredSymmAlg and a symmetric key derived from CA's private KAK and requester's public key	M	ref. B6
	Rand ::= SEQUENCE	M	
	int INTEGER	M	INTEGER "A"
	sender GeneralName	M	From PKIHeader, ref. 3.1.1
	POPODecKeyRespContent ::= SEQUENCE OF INTEGER	M	

SECTION	FEATURE	STATUS	REMARKS
	INTEGER "A" returned to sender	M	
	Use of POPOSigning Key structure	O	ref. CRMF, Alternative for demonstrating POP
	CA has a D-H certificate that is known to EE	M	
	alg field DHBasedMAC	M	
	signature field is MAC	M	
3.3	Operation-Specific Data Structures	M	
3.3.1	Initialization Request	O	Use for EEs first initializing into PKI
	PKIBody ::= ir [0] CertReqMessages	M	ref. CRMF for syntax Specifies the requested certificate(s)
	Template fields	M	
	SubjectPublicKeyInfo	O	ref. PKIX1, sec 4.1.2.7
	KeyId	O	ref. PKIX1, sec 4.2.1.1
	Validity	O	ref. PKIX1, sec 4.1.2.5
3.3.2	Initialization Responses	O	
	PKIBody ::= ip [1] CertRepMessages	M	ref 3.3.4
	Contains for each certificate request	M	
	PKIStatusInfo field	M	ref. 3.2.3
	Subject certificate	M	
	Private key	O	
	Encrypted with a session key	O	
	Encrypted with a protocolEncKey	O	
3.3.3	Registration/Certification Request	O	Used by existing PKI entities to obtain additional certificates
	PKIBody ::= cr [2] CertReqMessages	M	ref. CRMF for syntax
	Specifies requested certificates	M	
	Certificate requests for signing key pairs	O	NOT RECOMMENDED Legacy system interoperation only.
	PKIBody ::= p10cr [4] CertificationRequest	M	ref. PKCS #10
3.3.4	Registration/Certification Responses	O	
	Message contains	M	
	Status for each certificate requested	M	
	CA public key	O	
	Failure information	O	
	Subject Certificate	O	
	Encrypted private key	O	
	PKIBody ::= cp [3] CertRepMessages	M	ref 3.3.4
	CertRepMessages ::= SEQUENCE	M	
	caPubs [1] SEQUENCE SIZE OF	O	
	Certificate	M	ref. PKIX1, sec 4.1
	response SEQUENCE OF CertResponse	M	
	CertResponse ::= SEQUENCE	M	
	certReqId INTEGER	M	matches response to corresponding request
	Request had no certReqId value	C	
	value = -1	M	

SECTION	FEATURE	STATUS	REMARKS
	status PKIStatusInfo	M	ref. 3.2.3 Not present for some status values e.g. waiting, Others?
	only one failinfo field present in each CertResponse	M	
	certifiedKeyPair CertifiedKeyPair	O	Not present for some status values e.g. waiting, Others?
	CertifiedKeyPair ::= SEQUENCE	M	
	certOrEncCert CertOrEncCert	M	
	CertOrEncCert ::= CHOICE	M	
	certificate [0] Certificate	M	ref. PKIX1, sec 4.1
	only one present in each CertResponse	M	
	encryptedCert [1] EncryptedValue	M	ref. 3.2.2, CA returns the value of a certificate constrained so that only the intended recipient can obtain the certificate.
	privateKey [0] EncryptedValue	O	
	publicationInfo [1] PKIPublicationInfo	O	ref. 3.2.7
	rsplInfo OCTET STRING	O	ref. CRMF id-reqInfo-asciiPairs
3.3.5	Key Update Request Content	O	Used to request updates to non-revoked and valid certificates
	PKIBody ::= kur [7] CertReqMessages	M	ref. CRMF for syntax
	Template fields	M	
	SubjectPublicKeyInfo	O	ref. PKIX1, sec 4.1.2.7
	KeyId	O	ref. PKIX1, sec 4.2.1.1
	Validity	O	ref. PKIX1, sec 4.1.2.5
3.3.6	Key Update Response Content	O	
	PKIBody ::= kup [8] CertRepMessages	M	ref 3.3.4
	Contains for each key update requested	M	
	PKIStatusInfo field	M	ref. 3.2.3
	Subject certificate	M	
	Private key	O	
	Encrypted with a session key	O	
	Encrypted with a protocolEncKey	O	
3.3.7	Key Recovery Request Content	O	Request a certificate containing a signature public key.
	PKIBody ::= krr [9] CertReqMessages	M	ref. CRMF for syntax
	Template fields	M	
	SubjectPublicKeyInfo	O	ref. PKIX1, sec 4.1.2.7
	KeyId	O	ref. PKIX1, sec 4.2.1.1
3.3.8	Key Recovery Response Content	O	
	PKIBody ::= krp [10] KeyRecRepContent	M	
	KeyRecRepContent ::= SEQUENCE	M	
	status PKIStatusInfo	M	

SECTION	FEATURE	STATUS	REMARKS
	newSigCert [0] Certificate	O	ref. PKIX1, sec 4.1 Not present for some status fields. Which ones?
	caCerts [1] SEQUENCE SIZE OF Certificate	O	Not present for some status fields. Which ones?
		M	ref. PKIX1, sec 4.1
	keyPairHist [2] SEQUENCE SIZE OF CertifiedKeyPair	O	Not present for some status fields. Which ones?
		M	ref. 3.3.4
3.3.9	Revocation Request Content	O	
	Revocation of multiple certificates	O	
	sender field of PKIHeader contains requester	M	
	PKIBody ::= rr [11] RevReqContent	M	
	RevReqContent ::= SEQUENCE OF	M	
	RevDetails ::= SEQUENCE	M	
	certDetails CertTemplate	M	ref. CRMF for syntax Specifics of certificate being revoked.
	revocationReason ReasonFlags	O	ref. PKIX1, sec 4.2.1.13
	badSinceDate GeneralizedTime	O	ref. PKIX1, sec 4.1.2.5.2 Best knowledge of sender.
	crlEntryDetails Extensions	O	ref. PKIX1, sec 4.1 Requested crlEntryExtensions.
3.3.10	Revocation Response Content	O	Sent to revocation requester.
	A separate message also sent to subject of certificate revoked.	O	
	PKIBody ::= rp [12] RevRepContent	M	
	RevRepContent ::= SEQUENCE	M	
	status SEQUENCE SIZE (1..MAX) OF PKIStatusInfo	M	ref. 3.2.3 In same order as was sent in RevReqContent
	revCerts [0] SEQUENCE SIZE (1..MAX) OF CertId	O	ref. CRMF for syntax. IDs for which revocation was requested (same order as status).
	crls [1] SEQUENCE SIZE (1..MAX) OF CertificateList	O	ref. PKIX1, sec 5.1 The resulting CRLs (there may be more than one).
3.3.11	Cross Certification Request Content	O	
	PKIBody ::= ccr [13] CertReqMessages	M	ref. CRMF for syntax
	Requesting CA generates key pair	M	
	Requesting CA's private Key is not sent to responding CA	M	
3.3.12	Cross Certification Response Content	O	
	PKIBody ::= ccp [14] CertRepMessage	M	ref. 3.3.4
	No encrypted private key is sent	M	
3.3.13	CA Key Update Announcement Content	O	ref. 2.4 CA announces that it has updated its own key pair
	PKIBody ::= ckuann [15] CAKeyUpdAnnContent	M	

SECTION	FEATURE	STATUS	REMARKS
	CAKeyUpdAnnContent ::= SEQUENCE	M	
	oldwithNew Certificate	M	ref.PKIX1, sec. 4.1
	newwithOld Certificate	M	ref.PKIX1, sec. 4.1
	newwithNew Certificate	M	ref.PKIX1, sec. 4.1
3.3.14	Certificate Announcement	O	Publishes certificate(s) when there is no pre-existing method of publishing certificates. NOT RECOMMENDED when X.500 is the publication method.
	PKIBody ::= cann [16] CertAnnContent	M	
3.3.15	Revocation Announcement	O	CA announces immediate or pending certificate revocation
	CA warns certificate subject	O	Revocation request did not come from subject
	PKIBody ::= rann [17] RevAnnContent	M	
	status PKIStatus	M	ref. 3.2.3
	certID CertID	M	ref. CRMF for syntax
	willBeRevokedAt GeneralizedTime	M	ref. PKIX1, sec 4.1.2.5.2 Time that the new entry is entered into relevant CRLs
	badSinceDate GeneralizedTime	M	ref. PKIX1, sec 4.1.2.5.2
	crlDetails Extensions	O	ref. PKIX1, sec 4.1
3.3.16	CRL Announcement	O	CA issues new CRL(s)
	PKIBody ::= crlann [18] CRLAnnContent	M	
	CRLAnnContent ::= SEQUENCES OF CertificateList	M	ref. PKIX1, sec 5.1
3.3.17	PKI Confirmation Content	O	Final PKIMessage in three-way protocols. PKIHeader carries required information.
	PKIBody ::= conf [19] PKIConfirmContent	M	
	PKIConfirmContent ::= NULL	M	
3.3.18	PKI General Message Content	O	
	Useable by EE, RA, or CA	O	
	Receiver ignores unrecognized OIDs	O	
	Empty set sent from EE to CA	C	
	CA has no restrictions on information sent	M	
	Defines new CMP ReqMessages and RepMessages	O	Future needs or specific environments
	Defines new general purpose messages	O	Future needs or specific environments
	PKIBody ::= genm [21] GenMsgContent	M	
	GenMsgContent ::= SEQUENCE OF InfoTypeAndValue	M	
	InfoTypeAndValue ::= SEQUENCE	M	
	infoType OBJECT IDENTIFIER	M	
	infoValue ANY DEFINED BY infoType	O	Omitted for some infoTypes. Which ones?
3.3.19	PKI General Response Content	O	
	Receiver ignores unrecognized OIDs	O	

SECTION	FEATURE	STATUS	REMARKS
	PKIBody ::= genp [22] GenRepContent		
	GenRepContent ::= SEQUENCE OF InfoTypeAndValue	M	ref. 3.3.18
3.3.20	Error Message Content	O	
	PKIBody ::= error [23] ErrorMsgContent	M	
	ErrorMsgContent ::= SEQUENCE	M	
	pkIStatusInfo PKIStatusInfo	M	ref. 3.2.3
	errorCode INTEGER	O	Implementation specific error codes.
	errorDetails PKIFreeText	O	ref. 3.1.1 Implementation specific error details.
4	MANDATORY PKI MANAGEMENT FUNCTIONS	M	Describes constraints on the values in the PKI management message data structure and the PKI management operation event sequence
	EE implementations provides functionality	M	
	RA/CA implementations provides functionality	M	
4.1	Root CA Initialization	M	ref. 1.2.2, B3
	Self-certificate produced by new root CA	M	ref. 2.4.1
	Public key fingerprint produced by new root CA	M	For EEs that can not obtain self-certificate
	EE uses fingerprint to verify self-certificate	M	
	OOBCertHash data structure carries fingerprint	M	ref. 3.2.5
4.2	Root CA Key Update	M	ref. 2.4.1, B5
4.3	Subordinate CA Initialization	M	ref. 1.2.2, 4.4, 4.7
	Subordinate CA produces initial revocation list	M	
4.4	CRL Production	M	ref. 4.3
	CA establishes CRLs prior to issuing certificates	M	
4.5	PKI Information Request	M	ref. B6
	PKI requests CA for current status	O	
	CA provides requested information	M	
	CA provides error codes if information cannot be provided	M	
	PKIMessages used	O	ref. 3.1
	GenMsg requests	M	ref. 3.3.18
	GenRep responds	M	ref. 3.3.19
	ErrorMsg	M	ref. 3.3.20
	Message protection	M	
	PasswordBasedMAC	O	ref. 3.1.3
	Other authentication means	O	e.g., EE has certificate
4.6	Cross Certification	M	ref. B7
	Requester CA is subject of cross-certificate	M	
	Requester CA must initialize before requesting	M	
	Responder CA is issuer of cross-certificate	M	
4.6.1	One-way Request-Response Scheme	M	Creates only one cross-certificate. For responder CA to receive a certificate it must assume requester role.

SECTION	FEATURE	STATUS	REMARKS
	Two CAs participating can verify each other's signatures OR there is out-of-band verification of certification request origin	M	
	Responder CA generates authorization code	M	
	Authorization code passed to requester CA via out-of-band means	M	
	Requester CA generates a symmetric key based on the authentication code	M	
	Requester CA uses symmetric key to generate MACs on all messages	M	
	Requester CA generates a random number	M	What is the random number used for? The PBM salt value (ref. 3.1.3)?
	Requester CA sends ccr message	M	ref. 3.3.11
	All certificate fields must be specified	M	ref. PKIX1, sec 4.1
	Include BasicConstraints extension	M	ref. PKIX1,
	Message MAC protected	M	
	Responder CA checks protocol version of ccr message	M	
	Responder CA saves requester random number	M	
	Responder CA generates random number	M	See above?
	Responder CA validates MAC	M	What action is taken on failure?
	Responder CA generates requester certificate	M	
	Contains requester CA public key	M	
	Signed by responder CA signature private key	M	
	Responder CA archives certificate	O	
	Responder CA generates a symmetric key based on the authentication code	M	
	Responder CA uses symmetric key to generate MACs on all messages	M	
	Responder CA sends ccp message	M	ref. 3.3.12
	Contains responder CA verification certificate	O	
	Requester CA verifies this certificate	M	
	Message MAC protected	M	
	Requester CA checks own system against responder CA system time in ccp	M	What constitutes failure? What action is taken on failure?
	Requester CA checks random numbers in ccp	M	What constitutes failure? What action is taken on failure?
	Requester CA validates MAC in ccp	M	What action is taken on failure?
	Requester CA responds with PKIConfirm message	M	ref. 3.3.17
	Message MAC protected	M	
	Requester CA writes certificate to repository	M	
	Responder CA checks random numbers in PKIConfirm		What constitutes failure? What action is taken on failure?
	Responder CA validates MAC in PKIConfirm		What action is taken on failure?
4.7	End Entity Initialization	M	
	Retrieval of trust condition information	O	

SECTION	FEATURE	STATUS	REMARKS
	Out-of-band verification of other CA public keys	O	
4.7.1	Acquisition of PKI Information	M	
	Certifying CA	M	
	Current root-CA public key	O	
	Certification path from the root CA to the certifying CA with CRLs	O	
	Algorithms and parameters supported	M	
	Additional information	O	Established by policy.
	PKIMessages used to obtain information	O	ref. 3.1, 4.5
	GenMsg requests	M	ref. 3.3.18
	GenRep responds	M	ref. 3.3.19
	ErrorMsg	M	ref. 3.3.20
4.7.2	Out-of-Band Verification of Root-CA Key	M	
	EE has root CA public key	M	
	EE obtains root CA's self-certificate via out-of-band means	O	
4.8	Certificate Request	M	ref. B9
	EE uses cr message	M	ref. 3.3.3
	EE possesses a signing key pair	O	
	EE signs message with digital signature	M	
	CA responds with cp message	M	ref. 3.3.4
4.9	Key Update	M	ref. B10
	EE uses kur message	M	ref. 3.3.5
	EE possesses a signing key pair	O	
	EE signs message with digital signature	M	
	CA responds with kup message	M	ref. 3.3.6
5	TRANSPORTS		How PKI management messages are encapsulated in various transport mechanisms
	Transport security mechanisms	O	
	PKIProtection	M	ref. 3.1.3
5.1	File Based Protocol	O	Means for conveying PKI messages via file transport.
	Only one DER encoded PKI Message per file	M	
	No extraneous header information	M	
	No extraneous trailer information	M	
5.2	Direct TCP-Based Management Protocol	O	Means for conveying messages via simple TCP transport.
	EE or RA initiates transaction	O	
	EE or RA can poll for results	M	
	RA or CA has a listener process to accept PKI messages	M	
	Utilize port 829	M	
	Initiator creates transaction ID	M	
	Responder provides polling reference number	M	
	When multiple response messages are being sent, new polling reference numbers are provided after each message	M	
	After the final PKI response message no new polling reference number is provided	M	

SECTION	FEATURE	STATUS	REMARKS
	RA or CA initiates transaction	O	
	EE supplies a listener process or is supplied with a polling reference to pick up PKI message	M	
	Transaction Initiator/Responder use direct TCP-based PKI messages	M	
	Message syntax	M	
	length (32-bit integer),	M	number of octets in remainder of message, i.e. value octets plus 1
	network byte order	M	
	flag (8-bits),	M	
	value	M	
	msgReq	O	PKI message from initiator
	flag = '00'H	M	
	value = DER-encoded PKI message	M	
	pollRep	O	Response when no PKI message ready. Provides polling reference number and time interval to next pollReq.
	flag = '01'H	M	
	value	M	
	polling reference (32-bit integer)	M	
	time-to-check-back (32-bit integer)	M	
	seconds since 0000 700101 UTC	M	
	Response to msgReq	O	
	pollReq	O	Request for PKI Message response to initial request
	flag = '02'	M	
	value	M	
	polling reference (32-bit integer)	M	
	negPollRep	O	Last PKI message response sent, transaction complete
	flag = '03'	M	
	value = '00'H	M	
	Response to msgReq	O	
	Response to pollReq	O	
	partialMsgRep	O	Partial response to request with new polling reference number and time interval to next pollReq.
	flag = '04'H	M	
	value	M	
	next polling reference (32-bit integer)	M	
	time-to-check-back (32-bit integer)	M	
	seconds since 0000 700101 UTC	M	
	DER-encoded PKI message	M	
	Response to msgReq	O	
	Response to pollReq	O	
	finalMsgRep	O	Final response to request

SECTION	FEATURE	STATUS	REMARKS
	flag = '05'H	M	
	value = DER-encoded PKI message	M	
	Response to msgReq	O	
	Response to pollReq	O	
	errorMsgRep	O	TCP error detected
	flag = '06'H	M	
	human readable error message	M	
	Response to pollReq	O	
	PKIConfirm message	O	ref. 3.3.17
	Initiator send msgReq	M	
	Responder returns negPollRep	M	
5.3	Management Protocol via E-mail	O	Means for conveying ASN.1-encoded messages via simple Internet mail transport.
	MIME object	M	
	Content-type: application/pkixcmp	M	
	Content-Transfer-Encoding: base64	M	
	ASN.1 DER-encoded PKIX-CMP message, base64-encoded	M	
	MIME object	O	Legacy support.
	Content-type: application/x-pkixcmp	M	
	Content-Transfer-Encoding: base64	M	
	ASN.1 DER-encoded PKIX-CMP message, base64-encoded	M	
5.4	Management Protocol via HTTP	O	Means for conveying ASN.1-encoded messages via simple browser-server transport.
	MIME object	M	
	Content-type: application/pkixcmp	M	
	ASN.1 DER-encoded PKIX-CMP message	M	
	MIME object	O	Legacy support.
	Content-type: application/x-pkixcmp	M	
	ASN.1 DER-encoded PKIX-CMP message	M	
6	SECURITY CONSIDERATIONS	M	
	PKI entity decrypts a "ciphertext" challenge and returns "plaintext"	O	NOT RECOMMENDED. If other security failures occur, this could result in the compromise of the PKI entity's private key. This could subject other assurance services to attack.
B	PKI Management Message Profiles		
B2	Algorithm Use Profile		
B3	"Self-signed" Certificate		
B4	Proof of Possession Profile		
B5	Root CA Key Update		
B6	PKI Information Request/Response		
B7	Cross Certification Request/Response (1-way)		
B8	Initial Registration/Certification (Basic Authenticated Scheme)		

SECTION	FEATURE	STATUS	REMARKS
B9	Certificate Request		
B10	Key Update Request		

References

CRMF
PKIX1
PKIXLDAP

Document Point of Contact:

Defense Information Systems Agency
ATTN: JIEO-JEBBC (Gregor D. Scott)
Ft. Monmouth, NJ 07703-5613
USA
Voice: 732-427-6856
Fax: 732-532-0853
Email: scottg@ftm.disa.mil